D

■❋ Treasury Board   Conseil du Trésor

Circular No.: 1978-25

T.B. No.: 756662

File No.: 9108-6

Date: June 19, 1978

To: Deputy Heads of Departments
     and Heads of Agencies

Subject: Guide on EDP Administration

Circular Letter 1974-87, dated May 21, 1974 announced the publication of the Guide on EDP Administration for Departments and Agencies of the Government of Canada. Subsequent amendments were announced in Circular Letters 1976-10 (April 22, 1976), 1977-13 (March 10, 1977) and 1978-11 (March 16, 1978).

At its meeting of May 18, 1978, the Treasury Board approved a number of new measures affecting EDP processing requirements, as well as replacements for Chapters X and XI, entitled "Security in an EDP Environment" and "EDP Standards" respectively. Copies of the two chapters are attached.

As with the Guide on EDP Administration, the new requirements and revised chapters apply to all departments and agencies named in Schedules A and B of the Financial Administration Act and to branches designated as departments for the purposes of that Act. Chapter X also applies to agencies named in Schedule C.

Current EDP policy states that "the government will meet its needs for EDP services from the private sector,

Circulaire n°: 1978-25

C.T. n°: 756662

Dossier n°: 9108-6

Date: le 19 juin 1978

Aux: Sous-chefs de ministères et
      chefs d'organismes

Objet: Guide d'administration de
        l'informatique

La circulaire n° 1974-87 du 21 mai 1974 annonçait la publication du Guide d'administration de l'informatique pour les ministères et les organismes du gouvernement du Canada. Des modifications étaient par la suite annoncées dans les circulaires suivantes: 1976-10 du 22 avril 1976, 1977-13 du 10 mars 1977, et 1978-11 du 16 mars 1978.

À la réunion du 18 mai 1978, le Conseil du Trésor a approuvé un certain nombre de nouvelles mesures touchant les exigences de l'informatique ainsi que le remplacement des chapitres X et XI intitulés respectivement "Sécurité dans le milieu de l'informatique" et "Normes en informatique". Vous trouverez ci-jointes des copies des deux chapitres.

Tout comme le Guide d'administration de l'informatique, les nouvelles exigences ainsi que les nouveaux chapitres s'appliquent à l'ensemble des ministères et organismes énumérés dans les annexes A et B de la Loi sur l'administration financière ainsi qu'aux directions désignées comme étant des ministères aux fins de cette Loi. Le chapitre X s'applique également aux organismes énumérés à l'annexe C.

La politique actuelle de l'informatique stipule que "les besoins du gouvernement en services d'informatique seront couverts

except where it is in the public interest or is more economical to provide these services internally". The aim is to give every possible consideration to private sector participation in meeting the government's EDP processing requirements.

In support of the present policy, a number of new practices are to be introduced immediately in order to identify additional likely opportunities for using private sector EDP services. These practices are:

1. Departments must conduct a thorough documented analysis of private sector alternatives prior to the establishment of new in-house computer centres or the operation of major new applications on existing centres.

2. Departments must conduct a comprehensive evaluation of their computer centre(s) before any upgrading of, changes in, or renewal of contracts for equipment so as to limit the growth of existing centres and to ensure their continuing cost-effectiveness.

3. Departments must also ensure that the provision of EDP support to relocated or decentralized government operations is through local service bureaux, or facilities management contracts, in preference to the installation of new government computers.

The Treasury Board Secretariat will monitor departmental compliance with these measures. As well, it will periodically select departments for a full evaluation of existing facilities,

par le secteur privé, sauf lorsque c'est dans l'intérêt public ou qu'il est plus économique que ces services soient assurés par le gouvernement". Cette façon de faire a pour but d'accorder toute l'attention possible à la participation du secteur privé lorsqu'il s'agit de satisfaire aux exigences du gouvernement en matière d'informatique.

Pour appuyer la présente politique, il y aura mise en oeuvre immédiate d'un certain nombre de nouvelles pratiques visant à déterminer d'autres occasions qui permettraient d'avoir recours aux services informatiques du secteur privé. Les ministères doivent:

1. Effectuer une analyse poussée des solutions de rechange offertes par le secteur privé avant d'établir de nouveaux centres internes d'informatique ou de mettre en oeuvre dans les centres actuels de nouveaux systèmes importants.

2. Faire une évaluation globale de leur(s) centre(s) d'informatique avant d'améliorer, de modifier ou de renouveler les marchés de matériel de manière à restreindre la croissance des centres actuels et d'assurer leur rentabilité constante.

3. Veiller à ce que le soutien informatique aux services gouvernementaux décentralisés ou réinstallés soit dispensé à l'aide de bureaux de service locaux, ou de marchés de gestion des installations, au lieu d'amener le gouvernement à installer de nouveaux ordinateurs.

Le Secrétariat du Conseil du Trésor surveillera l'application de ces mesures par les ministères. De même, il choisira périodiquement des ministères dont les installations actuelles feront l'objet

in much the same way that significant EDP projects are now selected for monitoring.

The revision of Chapter X, "Security in an EDP Environment", was undertaken by the Royal Canadian Mounted Police (RCMP), which is responsible for the EDP Security Evaluation and Inspection Team (SEIT), with the assistance of the Information Systems Division and is based on the cumulative experience of SEIT and of departments since 1974. This revision was endorsed by the Interdepartmental Computer Security Panel, the Security Advisory Committee and the Advisory Committee on Information Systems.

Changes to Chapter X include a general strengthening and clarification of directives, and roles and responsibilities, and also include the requirement for departments to report to the RCMP on the implementation of SEIT recommendations, and for the RCMP to report annually to the Treasury Board Secretariat on the security status of EDP facilities serving the government.

The revision of Chapter XI, "EDP Standards", was developed by the Information Systems Division in conjunction with the Steering Committee of the Government EDP Standards Committee (GESC) and with the support of the GESC Secretariat. This revision was also endorsed by the Advisory Committee on Information Systems. Changes to Chapter XI include an expansion and reformatting of directives and guidelines, and the clarification of roles and responsibilities and of adoption and waiver procedures.

d'une évaluation globale, et ce un peu de la même manière dont il procède pour choisir les projets informatiques d'importance qui font l'objet de sa surveillance.

La révision du chapitre X intitulé "Sécurité dans le milieu de l'informatique" a été entreprise par la Gendarmerie royale du Canada (GRC), organisme chargé de l'Equipe d'inspection et d'évaluation de la sécurité en informatique (EIES), de concert avec la Division des systèmes d'information. Le travail s'appuie sur l'expérience que l'EIES et les ministères ont acquise depuis 1974. Cette révision a reçu l'approbation du Comité interministériel de la sécurité en informatique, du Comité consultatif de la sécurité et du Comité consultatif des systèmes d'information.

Les modifications apportées au chapitre X se traduisent par un renforcement et une clarification des directives, rôles et responsabilités; de plus, le chapitre indique que les ministères sont tenus de faire rapport à la GRC au sujet de la mise en oeuvre des recommandations de la EIES et que la GRC doit, tous les ans, faire rapport au Secrétariat du Conseil du Trésor au sujet du niveau de sécurité des installations informatiques mises au service du gouvernement.

La révision du chapitre XI intitulé "Normes en informatique" est le fruit du travail de la Division des systèmes d'information de concert avec le Comité directeur du Comité des normes gouvernementales en informatique (CNGI) et avec l'aide du secrétariat du CNGI. La présente révision a également reçu l'approbation du Comité consultatif des systèmes d'information. Les modifications apportées au chapitre XI sont les suivantes: - un élargissement et une nouvelle présentation des directives et des lignes directrices ainsi que la clarification des rôles et responsabilités et la précision des procédures d'adoption et de renonciation.
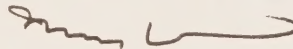
These two revisions to the Guide are the last to be published in the present format. The Guide will be republished in a standard format in 1979 as part of the Manuals on Administrative Policy which will integrate all Treasury Board administrative policies.

The measures detailed in this Circular Letter and the new chapters are effective immediately. Any enquiries should be directed to the Information Systems Division (telephone 992-1065).

Ces deux révisions du Guide sont les dernières qui seront publiées selon la présentation actuelle. En 1979, le Guide sera à nouveau publié, selon une présentation normalisée, dans le cadre des Manuels de la politique administrative qui renfermeront l'ensemble des politiques administratives du Conseil du Trésor.

Les mesures expliquées dans la présente circulaire ainsi que les nouveaux chapitres entrent en vigueur immédiatement. Pour de plus amples renseignements, il faut communiquer avec la Division des systèmes d'information, au numéro 992-1065.

Le sous-secrétaire
Direction de la politique administrative

Peter Meyboom
Deputy Secretary
Administrative Policy Branch

Attachments (2)

Pièces jointes (2)

Distribution/Diffusion: 1A, 1B, 2, 3A, 3B, 4
Internal/interne: 21A, 21B, 21D

GUIDE ON EDP ADMINISTRATION

SECURITY IN AN EDP ENVIRONMENT

PURPOSE

Deputy heads of departments and heads of agencies are responsible for establishing appropriate security measures within the departments and agencies of government. The purpose of this chapter is to provide guidance in the exercise of these responsibilities within the electronic data processing (EDP) environment. It is intended to assist those with a responsibility for the planning of security and the development of security procedures in an EDP environment.

Impenetrable security is generally thought to be unattainable. An optimum security system is one in which the cost of providing the security against a given threat in a given period has been balanced against the probability of the occurrence of the security infraction and the consequences, financial or otherwise, to the government if the security infraction occurs. This kind of balance should be achieved for all the differing threats to which information, personnel, or property can be subjected.

In most situations, particularly those in which governments find themselves, it is extremely difficult to determine either the probability of occurrence of a given threat, or the cost involved if the threat becomes a fact. Nonetheless, the importance of evaluating the possible threats and their impact before deciding on the security measures which are appropriate in any particular EDP environment cannot be overemphasized. In most cases it is possible to evaluate, within a factor of ten, both the expected frequency of occurrence and the cost associated with any defined threat. This will at least provide guidance on the appropriate emphasis of the security system.

Security threats are greatly dependent on the type of information being handled. Information which is being sought by a foreign power clearly warrants different protective measures from information which may be sought by a private citizen about a neighbour. Continuity of computer service is clearly more critical in support of some processes than for others. It is certain, however, that all data processing resources are worthy of at least a minimum level of protection. This chapter addresses the problem of minimum security standards and is therefore applicable to every data processing situation in government. In this respect, it should be pointed out that some departments need to impose more stringent rules than those contained herein.

Many aspects of security in an EDP environment are common to security in other environments. For these aspects established procedures and practices generally exist separately; such aspects are only briefly mentioned herein because guidance is readily available from departmental security officers and government agencies with specific security responsibilities.

This chapter was prepared with the assistance and concurrence of the Security Advisory Committee. It applies to agencies named in Schedule C of the Financial Administration Act, as well as to departments and agencies named in Schedules A and B, and to branches designated as departments for the purposes of the Act.

8.1   General security responsibilities and procedures in the EDP environment shall be those stated in the relevant departmental security manuals unless otherwise specified in these directives and guidelines. The provisions of this chapter will not apply to the Department of National Defence when inconsistent with the organization and operational needs of that Department as prescribed under the authority of the National Defence Act.

8.2   Departments and agencies using EDP facilities must ensure that:

(a)   information is classified or categorized in accordance with established procedures, and circumstances are specified under which data may be downgraded or declassified; and

(b)   all EDP facilities processing government information, including those under contract to the department or agency, meet specified security requirements.

8.3   Departments and agencies using EDP facilities, either government or private sector, which are engaged in handling information for the government must ensure that:

(a)   information in their custody, in whatever form, is protected to the level required by the relevant security classification or category and any accompanying caveats; and

(b)   an EDP security threat assessment is completed and an up-to-date threat evaluation report is prepared and maintained describing potential security risks of which account has been taken.

8.4   Any government organization planning the establishment, procurement, modification or relocation of a general purpose EDP facility, system, or service shall contact the departmental security officer (DSO) during the planning phase to ensure that all appropriate security authorities are consulted.

8.5   Departments and agencies must consult with the interdepartmental Security Evaluation and Inspection Team (SEIT) regarding the security status of their EDP facilities. Departments and agencies which have, or contemplate having, contracts that involve the processing of classified or otherwise sensitive information at a private sector EDP facility must contact the Security Branch of the Department of Supply and Services, who will arrange for the SEIT to inspect the facility and provide a security evaluation report.

8.6   Within six months of the receipt of a security evaluation report, the department or agency will advise the SEIT of the plan of action to deal with, and progress made against, outstanding problem areas identified in

the report. These progress reports shall be provided to the SEIT annually thereafter until all the recommendations have been addressed, or a re-inspection has been initiated.

8.7 The RCMP will compile an annual report to the Information Systems Division, Treasury Board Secretariat, on the security status of all EDP facilities serving the government. This report will be based on the results of all previous SEIT activities, and will take into account individual progress reported by departments and agencies during the reporting year.

GUIDELINES

8.8 All directors of EDP should designate an EDP security co-ordinator, who will receive direction from the DSO on security policy and report to the director of EDP on matters affecting EDP security. The security coor-dinator should be a senior staff member experienced in the EDP field, whose normal responsibilities require an understanding of EDP operations from both a management and a systems point of view. This individual should also have a general knowledge of security principles, procedures and problems.

8.9 The responsibilities of the EDP security co-ordinator should include:

(a) conducting regular security threat assessments and preparing evalua-tion reports;

(b) developing EDP security procedures, proposals for threat counter-measures, and contingency plans;

(c) periodically reviewing EDP security precautions and contingency plans;

(d) alerting the director of EDP to potential security problems;

(e) educating and motivating EDP personnel to observe security pre-cautions.

8.10 The EDP security evaluation report should be updated by the EDP security co-ordinator at annual intervals (or more frequently if occasion demands) and should provide the basis for modifications or additions to security measures affecting EDP activities.

8.11 The interconnection of EDP systems and telecommunications services should be carefully planned and co-ordinated to ensure that security of the information being processed and transmitted is provided. Advice in this regard should be requested from the appropriate authorities as indi-cated under "Role and Responsibilities", paragraphs 10 and 11.

8.12 All security criteria pertinent to an EDP job intended to be contracted should be included in any bid solicitation. Bidders should be evaluated on their responsiveness to the specified requirements.

8.13 The originator of the data to be processed should determine and clearly indicate the security classification or category of those data. The security marking of computer output is the joint responsibility of the originator and the EDP facility. The originator should ensure that the EDP facility manager is aware of the security requirements of the output. The EDP facility manager is responsible for the labelling and protection of the computer output as instructed by the originator.

8.14 Control measures for data input, processing, storage and output, program generation and maintenance, and hardware operation and support should be clearly identified in the standard operating procedures of the EDP facility.

ROLES AND RESPONSIBILITIES

A number of organizations and entities have responsibility for various aspects of security in the Government of Canada. Many of the security responsibilities indicated below are not specific to EDP, but they are listed here for reader convenience. This section is included only to serve as a quick reference and is not intended as an authoritative source.

1. **Deputy Ministers and Heads of Agencies**

   Deputy ministers and heads of agencies are solely responsible for implementation and administration, within their department or agency, of government security policies and procedures as set out in references 1 and 2. This includes responsibility for determining the level of security required by EDP services employed to process the work of their departments and agencies.

2. **Departmental Security Officers (DSO)**

   The departmental security officer is responsible to the deputy minister or head of agency, for ensuring the implementation, co-ordination, supervision and audit of all security policies, standards and procedures, including those that affect EDP within his department.

3. **Security Advisory Committee (SAC)**

   The Security Advisory Committee is an interdepartmental body which provides advice on security matters, and counsel and guidance for the resolution of security-related conflicts within the government.

4.   **Interdepartmental Computer Security Panel (ICSP)**

The Interdepartmental Computer Security Panel is an advisory body reporting to the SAC and consisting of representation from selected government centres of EDP. It is responsible for making recommendations and providing advice on security issues relating to EDP practices, and for reviewing and advising on the activities of SEIT.

5.   **Communications - Electronic Security Committee (CSC)**

The Communications - Electronic Security Committee is an interdepartmental advisory body reporting to the SAC on the security of government communications.

6.   **Security Equipment Advisory Committee (SEAC)**

The Security Equipment Advisory Committee is an interdepartmental committee reporting to the SAC and is responsible for all matters relating to the provision of approved physical security equipment for government use.

7.   **Royal Canadian Mounted Police (RCMP)**

The Commissioner, Royal Canadian Mounted Police, is responsible for advising deputy ministers and heads of agencies on the implementation of government security policies as outlined in directives, regulations and instructions, consistent with responsibilities allocated in these directives and guidelines. He may obtain assistance for certain aspects of this responsibility from other departments and agencies within government as mutually agreed upon.

The Commissioner, RCMP, is responsible for the organization and operation of the Security Evaluation and Inspection Team (SEIT).

8.   **EDP Security Evaluation and Inspection Teams (SEIT)**

The Security Evaluation and Inspection Team, organized and administered by the RCMP in accordance with the provisions of this guide, and drawing upon interdepartmental resources when practical, is responsible for conducting inspections and evaluations of government EDP facilities as well as private sector facilities engaged in processing government information under contract.

9.   **Department of Supply and Services (DSS)**

The Department of Supply and Services is responsible for the supply of, and contractual agreements for, all EDP equipment and services to be used by government departments and agencies. This includes ensuring that suppliers of equipment have incorporated into the manufacture and design of any equipment, all security specifications as established by government security regulations and guidelines. DSS is also responsible for arranging for the security clearance of private sector facilities and personnel, and for arranging the SEIT inspections of private sector EDP facilities.

10. **Communications Security Establishment (CSE)**

The Communications Security Establishment of the Department of National Defence has been designated as the national COMSEC agency and, as such, is responsible for the provision of guidance and advice on communications-electronic security (COMSEC) matters to all departments and agencies of the government. The Departments of External Affairs, National Defence, Communications, Supply and Services, and Transport, as well as the Royal Canadian Mounted Police and the Privy Council Office, will deal directly with CSE on COMSEC matters. All other departments and agencies will follow the procedures set out in paragraph 11 below.

11. **Department of Communications (DOC)**

The Department of Communications is responsible for providing guidance and advice on COMSEC matters to all departments and agencies not represented on the CSC. In addition, with respect to all departments and agencies, the DOC is responsible for providing other services within the intent of the Treasury Board document *Guide on Telecommunications Administration* (December 1976).

12. **Department of Public Works (DPW)**

Whenever the Department of Public Works is responsible for the construction of, or structual changes to, a building, it is also responsible for implementing structural requirements dictated by security standards. This includes application of the federal, provincial or municipal building codes and fire regulations, and consultation with the RCMP as to their effect on security requirements.

INTERPRETATION AND ADVICE

It is the responsibility of the Security Evaluation and Inspection Team of the RCMP to evaluate the status of security in government EDP operations. This they do through regular inspections of the facilities used by the various departments and agencies. The frequency of inspection of a given facility depends on the sensitivity of the data and information processed, and how critical the service provided is in relation to overall government objectives and priorities.

Following inspection of a facility, the SEIT will prepare an evaluation report for the deputy head in charge of the facility indicating the classification level or category of information which SEIT considers the facility can handle and process securely. Copies of the evaluation report will also be provided to the DSO, and the responsible director(s) of EDP.

In the case of private sector facilities under contract, an evaluation report will be provided for the Director, Security Branch, DSS who will subsequently make the results available to the chief officer of the private sector organization. These results are made available by DSS to departments and agencies contracting for EDP services from the subject facility, on request.

Copies of all SEIT reports will be made available to the Director, Information Systems Division, Treasury Board Secretariat, and the Chairman, Security Advisory Committee, on request.

Within sixty days of delivery of a security evaluation report, the SEIT will contact the DSO of the subject department or agency to provide interpretation and advice on observations and recommendations as necessary. This should lead to the formulation of an action plan on the part of facility management and security personnel to address outstanding security problems and recommendations of the report.

The rating criteria used for EDP security evaluations are the EDP Security Standards prepared under the direction of the ICSP, and in consultation with the Government EDP Standards Committee.

REFERENCES

1. *Security of Information in the Public Service of Canada,* (Confidential), Office of the Privy Council, November 1956.

2. *Official Secrets Act* (R.S.C. 1970, Chapter 0 - 3).

3. *Guide on Telecommunications Administration,* Treasury Board, December 1976.

EDP STANDARDS

APPENDICES

XI-1. RELEVANT INTERNATIONAL ORGANIZATION FOR
        STANDARDIZATION (ISD) COMMITTEES, SUB-COMMITTEES
        AND WORKING GROUPS.

XI-2. LIST OF DEPARTMENTS OR AGENCIES WITH MEMBERSHIP
        ON THE GOVERNMENT EDP STANDARDS COMMITTEE

EDP STANDARDS

PURPOSE

The EDP policy approved by the Treasury Board promotes the preparation, publication and adoption of standards for an orderly and coherent growth of computer-related work in Canada. This chapter identifies the general area encompassed by the standards program and indicates the processes whereby it is administered. In general the area of activity corresponds to that covered by the International Organization for Standardization (ISO) technical committee (Computers and Information Processing) (see Appendix XI-1).

To further the attainment of the basic objectives of the standards program the Treasury Board Secretariat, in consultation with the Advisory Committee on Information Systems, has established a Government EDP Standards Committee (GESC). This committee is responsible for co-ordination of the work of federal government officers in national and international agencies concerned with EDP standards, and for the development of EDP standards required for the federal public service where suitable national or international standards do not exist. In the exercise of its responsibilities the GESC is concerned with the promotion and issue of three different types of standards documents:

Treasury Board Approved EDP Standards
GESC Recommended EDP Standards
GESC Guidelines.

DIRECTIVES

9.1   The GESC shall submit through the Advisory Committee on Information Systems any EDP standard endorsed by both committees for subsequent approval by the Treasury Board.

9.2   Departments and agencies of the federal government shall comply with Treasury Board Approved EDP standards, except in cases where:

(a)   special conditions justify deviations therefrom;

(b)   discussions with the GESC Secretariat and (where appropriate) the Steering Committee, including suggestions for revision of the standard, have failed to resolve the issue; and

(c)   both the Information Systems Division of the Treasury Board Secretariat and the GESC Secretariat have been informed by memorandum from the Deputy Head of the conditions pertaining to, and the expected duration of, the deviation.

9.3   The Government EDP Standards Committee shall approve and issue, through the GESC Secretariat, GESC Recommended EDP standards which have been endorsed by the Advisory Committee on Information Systems (ACIS).

9.4 Departments and agencies of the federal government shall adhere to GESC Recommended EDP standards, except in cases where:

(a) discussions with the GESC Secretariat and (where appropriate) the Steering Committee, including suggestions for revision of the standard, have failed to resolve the issue; and

(b) the GESC Secretariat has been informed by memorandum of the reasons for non-compliance.

9.5 Standards for security in the EDP Environment, which are exempt from the adoption procedures described elsewhere in this chapter, shall be developed and recommended by the Commissioner, R.C.M.P., with the assistance of the Inter-departmental Computer Security Panel; and shall be reviewed by the Advisory Committee on Information Systems and the Security Advisory Committee prior to Treasury Board approval and promulgation by the Government EDP Standards Committee.

GUIDELINES

9.6 The Government EDP Standards Steering Committee may from time to time issue GESC Guidelines. These will provide a formal mechanism whereby generally accepted good practices relative to EDP can be brought to the attention of departments or agencies.

9.7 Departments and agencies of the federal government are recommended to adhere to the practices, methods or ideas expounded in the GESC Guidelines wherever such compliance is feasible.

A. BACKGROUND

EDP standards, to be truly effective, must take into account that work takes place at three separate levels, with somewhat differing characteristics at each level. These are:

— the individual department, EDP centre or business establishment;

— the federal or provincial governments, or a corporation operating major facilities at several locations;

— the national or international level.

EDP standards are often developed by an individual department, EDP centre or business establishment to deal with specific problems of the agency. They are, in consequence, likely to be enforced by line authority.

Many corporations or governments which operate major EDP facilities at several locations have developed EDP standards to govern EDP work at all of these locations. These standards are likely to deal with problems common to many or most locations, such as interchange of information, programs or staff.

The extent to which such corporate EDP standards are enforced by line authority depends on specific business or government administrative policy. Where they exist, they exert a considerable influence on the in-house standards developed at particular locations.

The national and international level of EDP standards work is characterized by a genuine effort to develop a full consensus among all interests affected by a proposed standard. Where such standards can be developed they are most valuable, but the fact that they must rest on full consensus does restrict the areas in which standards can be formulated. In general, there is no "line authority" to enforce these standards, although in some areas international standards have become of prime interest to national regulatory agencies who can readily ensure compliance (e.g. Communications).

The Government EDP Standards Committee is established to deal with the middle level of EDP standards activity. It also has the responsibility for developing a Canadian government outlook with respect to the EDP activities of national and international standards agencies, including the initiation of requests for new standards and the establishment of a co-ordinated federal government position with respect to standards put forward by these agencies for adoption.

The EDP standards program should not duplicate the work of government regulatory agencies which have responsibility in particular fields. Nonetheless, the GESC may make representation to regulatory agencies in cases where existing regulations do not appear to be fully consistent with desirable EDP standards, and may publicize new or existing standards and guidelines within the government EDP community and explain their relevance to EDP work.

B. DEFINITIONS

1. A Standard

The Standards Council of Canada defines a standard as the approved rules for an orderly approach to a specific activity. The Canadian Standards Association defines a standard as a thing, a feature, a method, or a process which is recognized as or agreed to be a model for imitation.

A standard is normally exactly specified and approved by a recognized authority after consultation among prospective users and suppliers, and embodies the degree of consensus achievable at the time it is prepared. A standard differs from a directive or guideline in that its subject matter is normally technically oriented rather than administratively oriented.

2. Treasury Board Approved EDP Standards

A Treasury Board Approved EDP Standard is an EDP standard which has been accepted by the Government EDP Standards Committee, endorsed by the Advisory Committee on Information Systems and then approved by the Treasury Board. Treasury Board approval will usually be based on one of the following grounds:

adoption of the standard will result in a significant net saving to the government;

adoption of the standard will further government policies and objectives in a cost-effective manner.

3. GESC Recommended EDP Standards

A GESC Recommended EDP standard is a standard accepted for issue by the GESC, which has been endorsed by the Advisory Committee on Information Systems but for which no formal approval by the Treasury Board has been requested.

4. GESC Guidelines

GESC Guidelines are approved and issued by the GESC Steering Committee. They provide a means of disseminating information on generally accepted good practices, methods or ideas.

C. ROLES AND RESPONSIBILITIES

1. Standards Council of Canada (SCC)

The SCC is the national standards body of Canada. Its purpose is to foster and promote voluntary standardization in Canada, to accredit standards writing organizations and, as appropriate, to approve standards produced by these organizations as National Standards. The SCC promotes Canadian participation and represents Canada in international standardization activity through membership in such international bodies as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

2. Canadian Standards Association (CSA)

The CSA is the SCC-accredited Canadian body for the development and approval of Canada-wide EDP software standards (and for standards in many non-EDP fields). The CSA also serves as the secretariat to Canadian Advisory Committee on certain ISO committee and sub-committees concerned with EDP standards. The committee of CSA which manages and co-ordinates these tasks is the Sectional Committee for Computers, Information Processing and Office Machines (CIPOM) and its associated sub-committees and working groups. No Canadian body has yet been accredited for the development and approval of EDP hardware standards.

3. Canadian Government Specifications Board (CGSB)

The CGSB is the principal federal government standards writing agency, and is accredited by the SCC to develop and approve national standards in many fields. It is responsible for the Secretariat of the Canadian Advisory Committee on TC 154 (Documents and Data Elements in Administration, Commerce and Industry) which deals with many EDP-related areas of standardization.

4. Government EDP Standards Committee (GESC)

The GESC is responsible for appraising EDP standards proposed for general federal government use and for recommending which EDP standards should receive Treasury Board approval. In addition, through the office of its chairman, it directs the work of the GESC Secretariat.

A more detailed outline of the responsibilities of the GESC, the GESC Steering Committee and the GESC secretariat is provided in Section D following.

5. **Department of Supply and Services (DSS) — Services**

The chairmanship of the GESC and that of GESC/SC reside within the DSS (Services) administration, which is responsible for providing a secretariat to the GESC.

6. **Department of Supply and Services (DSS) — Supply**

As the department responsible for the acquisition of EDP and other goods and services in the Canadian government, DSS has a particular interest in EDP standards development as a means to assist it in the development of clear, consistent specifications for goods and services to be acquired.

7. **Department of Communications**

The Department of Communications has responsibilities for administering and ratifying Canadian telecommunications regulations, and for representing Canada in the International Telegraph and Telephone Consultative Committee (CCITT) for the International Telecommunications Union (ITU).

8. **Royal Canadian Mounted Police (R.C.M.P.)**

The Commissioner, R.C.M.P., is responsible for developing and recommending security standards for application to EDP in government usage. These standards are developed with the assistance of the Interdepartmental Computer Security Panel, and in consultation with the GESC.

D. **THE GOVERNMENT EDP STANDARDS COMMITTEE (GESC)**

1. **Objectives**

The overall objectives of the GESC are the co-ordination of the participation of federal government officers in national and international EDP standards work, and the development, approval and implementation of EDP standards in the federal public service. In pursuance of these objectives, the committee is expected to work with and through accredited standards agencies to the fullest practical extent.

2. **Membership and Organization**

(a) Members

There will be two groups of members in the GESC: ex-officio and individual. The ex-officio members will include:

i.   a member named to represent each of the major users of EDP identified in Appendix XI-2;

ii. a member named to represent each of the Department of Communications, the Supply Administration of the Department of Supply and Services, the Security Systems Branch of the R.C.M.P., and the Treasury Board Secretariat;

iii.   the Chairman of the GESC (if not already a member);

iv.   an individual recommended by any department or the GESC (and approved by the Advisory Committee on Information Systems) to represent a department not otherwise represented on the Committee;

The individual members will include any individual public servant elected to the Committee by the existing membership of GESC because of his interest in and contribution to standards work in the federal government.

The members of the GESC will:

—   elect members to the elective positions on the Steering Committee of the GESC;

—   elect individual members to the GESC;

—   recommend EDP standards projects to the Steering Committee, and assist in staffing approved projects;

—   approve the program of EDP standards work recommended by the Steering Committee;

—   provide comments on draft standards circulated by the GESC Secretariat;

—   vote on EDP standards to be recommended for Treasury Board approval or to be adopted as GESC Recommended EDP standards;

—   provide information to the GESC Secretariat regarding the extent to which EDP standards are being observed within government organizations.

(b)   Steering Committee

The Steering Committee of the GESC will consist of:

—   the representatives named as GESC members under subsection 2.(a)ii above;

—   three members elected by the membership of the GESC for a maximum three-year term, with one to be replaced each year;

—   the chairman of the GESC.

The Steering Committee will:

—   initiate the development of EDP standards within the Public Service as necessary;

—   develop and forward to the CSA, or any other organization accredited by the Standards Council of Canada as part of the national standards system, by whatever means are appropriate, the Canadian government position on the needs for particular EDP standards, on proposed EDP standards and on any other EDP matters put forward for discussion or resolution;

—   prepare a program of EDP standards work for approval by the GESC;

—   organize and approve terms of reference for and membership of working groups for proposed EDP standards projects when the accredited standards agency can not give these early attention, or the need is specific to the federal public service;

—   arrange for appropriate Canadian government representation on CIPOM and its working groups, and on any other accredited EDP standards agency;

—   determine when proposed standards should be submitted to members for comment or approval;

—   submit to the Advisory Committee on Information Systems all EDP standards which should receive Treasury Board approval and all GESC recommended EDP standards;

—   approve GESC Guidelines for issue by the Secretariat;

—   approve the EDP Standards Directory and its updates as prepared by the GESC Secretariat.

(c)   Chairman

The chairman of the GESC is appointed from within the DSS (Services) administration by the Treasury Board, after consultation with the Advisory Committee on Information Systems. The chairman is responsible for:

—   directing the work of the GESC Secretariat;

—   calling and presiding over meetings of the Steering Committee and the GESC;

—   appointing a vice-chairman for the members of the Steering Committee, to act for him in his absence.

3.   **The GESC Secretariat**

The secretary to the GESC, and any other staff who may be required, will be provided by DSS (Services), and will be under the direction of the chairman of the GESC. The appointment of a new secretary must be approved by the chairman of the GESC.

The Secretariat is responsible for:

— taking minutes at meetings of the GESC;

— circulating information (e.g. draft standards, notice of meetings, minutes, current membership mailing lists, etc.) to members of the Steering Committee and the GESC;

— undertaking or arranging for research in connection with EDP standards development as directed by the chairman of the GESC;

— arranging for the publication and distribution to government departments of a directory of Treasury Board approved and GESC recommended EDP standards, and GESC guidelines, and maintaining an awareness of the degree of compliance with each standard;

— maintaining source files on EDP standards and relevant departmental practices for the use of any federal government employee who needs access to such information, and giving assistance in the finding of required information.

4. Meetings of the Steering Committee and the GESC

Meetings of the Steering Committee will be held at the discretion of the chairman of the GESC, but should take place at least twice a year. Meetings of the GESC will also be at the discretion of the chairman, but should take place at least once a year.

E. DEVELOPMENT AND ADOPTION OF STANDARDS

1. Development of Standards

Wherever feasible, the standards of the International Organization for Standardization (ISO), or the National Standards of Canada, or standards developed by an accredited EDP standards agency, will be adopted as federal government EDP standards. The GESC will endeavour to work with accredited agencies on standards development. From time to time it may be necessary to proceed with the development of standards independent of accredited agencies, but in general this should happen only when the need is specific to the federal public service, or when the accredited agency cannot give sufficient priority to a proposal.

Any member of the GESC may recommend an EDP standards project to the Steering Committee, and may propose amendments to the program of work submitted by the Steering Committee in the event that some recommendations are not included, or are not given sufficient priority.

The Steering Committee will normally convene working groups to undertake specific tasks of defining requirements for standards, reviewing EDP standards produced by other standards bodies, participating in the work of other EDP standards bodies, developing EDP standards based on approved requirements when this task cannot be undertaken by an accredited standards agency,

and other matters. A working group may consist of one or several experts, and will exist only until the completion of its assigned task. Working groups may include industry representatives or other members of the public as appropriate.

Whether the standards development work directly supports an accredited standards agency or is independent, it is expected that work of this type undertaken in the government will normally be voluntary, and with the assent of the volunteer's supervisor. The GESC Secretariat will provide support and assistance as far as its resources permit.

2. Adoption of Standards

Before a draft EDP standard can be recommended for Treasury Board approval or adopted as a GESC recommended EDP standard the following procedures must be followed:

— the Steering Committee must approve a copy of the draft standard for circulation to all members of the GESC, giving them 30 days from date of mailing to submit written comments;

— the written comments must be mailed to all members of the GESC at least 15 days before the meeting at which the standard(s) will be considered for adoption, or 15 days before the due date for a write-in vote.

If, as a result of the comments received, substantive changes are made to the standard, the Steering Committee may recirculate the revised draft to all members for further comment.

If any two members of the Steering Committee request a meeting to approve a standard, approval may not take place by letter ballot. However, members absent from approval meetings may register their vote by mail, or may appoint a proxy to represent them at the meeting and vote on their behalf.

The following vote table shall be used to determine adequate support for either a GESC recommended EDP standard, or an EDP standard which is to be submitted for the approval of the Treasury Board.

Minimum Number of Affirmative Votes Required

Number of Members Voting (a)	For adoption of a GESC Recommended EDP Standard	For recommendation as an EDP Standard to be submitted for Treasury Board approval (b)
33	20	30
32	19	29
31	18	28
30	18	27
29	17	26
28	16	25
27	16	24
26	15	23
25	15	22
24	14	21
23	13	20
22	13	19
21	12	18
20	12	17
19	11	16
18	10	15
17	10	14

NOTE: (a) At least two-thirds of current membership must vote.

(b) Must be identified as a potential Approval Standard before the vote is taken.

RELEVANT INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) COMMITTEES SUB-COMMITTEES AND WORKING GROUPS

The following ISO committees, sub-committees (SC) and working groups (WG) were in existence in December, 1973, and are either directly concerned with EDP standards development or related to it.

1.   Technical Committee 97 — Computers and Information Processing

    a.   Abridged scope

        Standardization in the area of computers and associated information processing systems and peripheral equipment, devices and media relating thereto.

    b.   Subordinate committees and working groups

SC 1	Vocabulary
— WG 1	Maintenance
— WG 2	Editing
SC 2	Character sets and coding
SC 3	Character and Mark recognition
SC 5	Programming language
— WG 1	Programming languages for the control of industrial process (PLIP)
— WG 2	Graphics
— WG 3	Data base management systems
SC 6	Data communications
— WG 1	Data communications control procedures
— WG 2	Public data networks
— WG 3	Physical interface characteristics
SC 7	Design and documentation of computer-based information systems
— WG 1	Symbols and conventions for flowcharts
— WG 2	Rules for documentation of information processing systems
— WG 3	Program design
— WG 4	Decision tables
SC 8	Numerical control of machines
SC 9	Programming languages for numerical control
— WG 1	Input language
— WG 2	CLADATA
— WG 3	Technology description

SC 10	Magnetic discs
SC 11	Computer magnetic tape
SC 12	Instrumentation magnetic tape
SC 13	Interconnection of equipment
— WG 1	Process interfaces for computer systems
— WG 2	Interface standards administration
— WG 3	Lower-level interface functional requirements and lower-level interfaces
SC 14	Representations of data elements
-- WG 1	Standardization guidelines for the representation of data elements
SC 15	Labelling and file structure
WG 1	Flexible disks
— WG 2	Data communications liaison
SC 16	Open system architecture

2. Technical Committee 95 — Office Machines

  a. Abridged scope

  Standardization on terminology and definitions of functions of office machines and other fundamental elements of interest to users and manufacturers of such machines.

  NOTE: Although this program may seem anomalous, much of this area concerns machine readable data preparation and the characteristics of computer peripherals and ancillaries such as keyboards and computer line printers.

  b. Subordinate committees and working groups

SC 4	Duplicating and document copying machines
— WG 1	Dimensional aspects of attachment features of duplicating stencils
-- WG 2	Terminology of duplicators and document copying machines
SC 5	Dictation machines
- WG 1	Terminology of dictation equipment
SC 6	Mail processing machines and other special machines
SC 7	Vocabulary, classification and identification of office machines

SC 9	Interrelation between office machines and forms
— WG 2	Character and line spacings
— WG 3	Requirements for paper for continuous forms
SC 12	Printing ribbons and their accessories
— WG 1	Specifications of spools
SC 14	Keyboard arrangements
SC 15	Numeric and alphanumeric office machines
— WG 1	Electronic calculators
SC 16	Symbols used on office machines
— WG 1	Preparatory work
SC 17	"Credit cards" and identification cards
— WG 1	Identification cards
— WG 2	Machine readable techniques
— WG	Registration authority group (RAG)

3. Technical Committee 46 — Documentation

   a. Abridged scope

   Standardization in the field of documentation, libraries and related information handling, including information systems and interchange networks as applied to documentation.

   b. Subordinate committees and working groups

— WG 1	International standard book numbering
— WG 2	Representation and coding of country names
— WG 3	Terminology of documentation
— WG 5	Guidelines for the establishment of thesauri
— WG 6	Bibliographic description
— WG 7	Presentation of publications
SC 1	Documentary reproduction
— WG 1	Microfiches
— WG 2	Microcopying of technical drawings
— WG 3	Microcopying newspapers
— WG 4	Quality of microcopies
— WG 5	Vocabulary
SC 2	Conversion of written languages
SC 4	Automation in documentation
— WG 1	Character sets
— WG 2	Content designators
— WG 3	Bibliographic filing arrangements for catalogues

4. Technical Committee 154 — Documents and Data Elements in Administration, Commerce and Industry

    a. Abridged scope

        Standardization of layout, formats and representation of data used for information interchange within administration, commerce and industry.

        NOTE: The word "document" is understood, as defined by TC46 and TC 97, to be "a data medium with data recorded on it that generally has permanence and that can be read by man or machine."

    b. Subordinate committees and working groups

SC 1	Terminology
SC 2	Documents
SC 3	Data elements
SC 4	Filing

LIST OF DEPARTMENTS OR AGENCIES
WITH MEMBERSHIP ON THE
GOVERNMENT EDP STANDARDS COMMITTEE

Agriculture
Employment and Immigration Commission
Energy, Mines and Resources
Fisheries & Environment
Industry, Trade and Commerce
National Defence
National Health and Welfare
National Library
National Research Council
National Revenue — Customs and Excise
National Revenue — Taxation
Post Office
Public Archives of Canada
Public Service Commission
Public Works
Royal Canadian Mounted Police
Statistics Canada
Supply and Services — Services
Supply and Services — Supply (Printing & Publishing)
Supply and Services — Supply (Systems & Services)
Transport
Employment and Immigration Commission